

# Bitcoin – základy a stavební kameny

Co o něm nevíte a neměli jste se koho zeptat...

Karel Fillner  
cointelegraph.cz



# Bitcoin v očích veřejnosti a médií



# Co je bitcoin doopravdy

- Satoshi Nakamoto – 2009 (předtím např. Egold 1996 USA, centralizovaný projekt). Nutnost důvěřovat prostředníkům je nahrazena kryptografií a P2P
- Decentralizovaná peer to peer síť (Bitcoin vs. bitcoin)
- Open-source program a komunitní projekt
- Projekt krytý největší výpočetní silou
- Pseudonymní digitální měna (komodita?)
- Internet 2.0 - Money 2.0





# FIAT vs. BITCOIN



- FIAT – měna s nuceným oběhem, zákonná měna
- Bitcoin - měna spravovaná bez centrální autority
- Pilířem je státní monopol a garance vlády a CB
- Pilířem jsou matematické zákony a výpočetní síla
- Lze je dotisknout, devalvovat, znárodnit
- Postupně uvolňovaný přesný počet 21 milionů
- Účty lze obstatit, zabavit x BTC adresa je skrytá
- Fin. transakce jsou vratné x BTC transakce nevratné
- Kvalitní padělky lze těžko rozeznat x Nelze je padělat

# Praktické vlastnosti bitcoinu

- Založení účtu nic nestojí, neomezený počet adres
- Vlastník bitcoinů není známý, pokud sám nechce
- Účty a transakce jsou však veřejné a dohledatelné
- Pro přijímání bitcoinů není nutný internet
- Transakce nelze změnit, vrátit ani jim zabránit
- Poplatky jsou levné pro libovolnou částku
- Bitcoinovou sítí lze nahradit registry a ověřovací autority – notář, katastr, pravost zboží, volby

## How Bitcoin Works

sender sends bitcoin to receiver; miner validates the transaction and records it to the blockchain....

18BSM9B1dZTMGcLfs2Dck868fjgwrwhjk4



sender



miner

receiver gets bitcoin from sender and can spend it after the blockchain is confirmed by other miners....

14MLqx6LeKZkxPSaKPxyekM4Nh77P1CiQ1



receiver



blockchain

anyone can see the transaction in the blockchain.... [www.blockchain.info](http://www.blockchain.info)



anyone



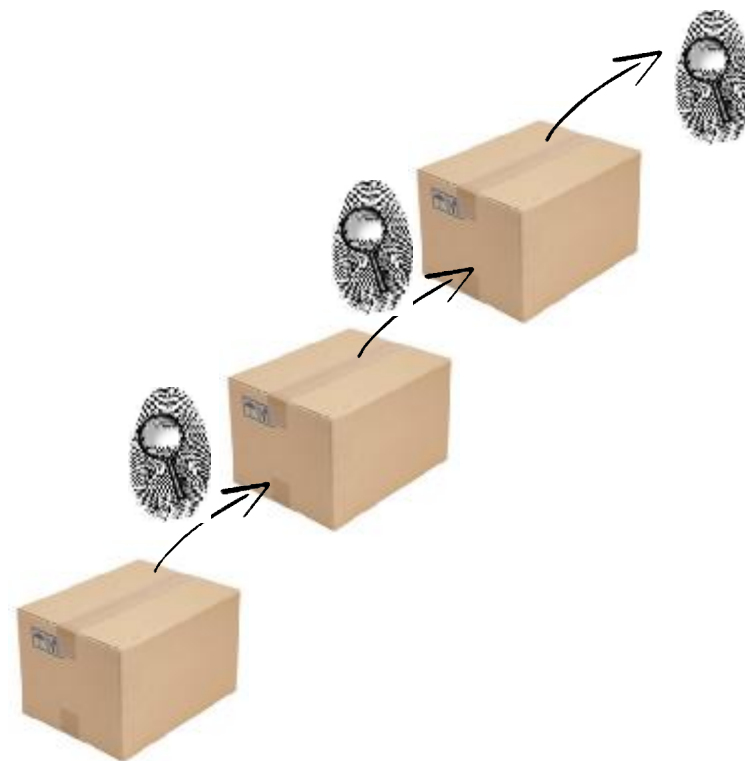
# Jak probíhají transakce a mining

## Potvrzení transakce – časové razítko na bloku + 25 BTC odměna



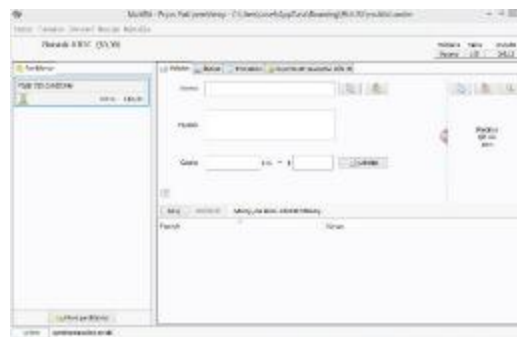
Hash:  
0x000000000000000015e30e78a09861d  
e434a999d82fc43ad5231e7d58fce81d4

Blockchain – 1 blok cca 10 minut,  
difficulty - samoregulace



# Bitcoin adresa a peněženka

- Bitcoin adresa: 14MLqx6LeKZkxPSaKPxyekM4Nh77P1CiQ1
- Online peněženky – Coinbase, Blockchain.info
- Softwarové peněženky – Bitcoin QT, Electrum, Multibit (liší se také v načítání blockchainu)
- Hardwarové peněženky – např. TREZOR





# Mobilní peněženky



Mycelium



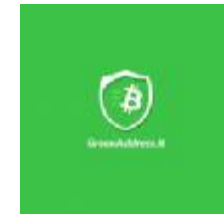
Blockchain



bitWallet



CoinPocket



Green Address

## Paper wallets



# Kde se dá bitcoin koupit a prodat

## Burzy a směnárný

ČR – BitStock vs. Simplecoin

Evropa – Bitstamp , btc-e (Bulharsko)

USA – Bitfinex, Kraken, Coinbase

Čína – BTCChina, OkCoin, Huobi (až 70% trhu)

Altcoin burzy – Cryptsy.com, Bittrex

## Bitcoinové bankomaty

Klientské centrum Praha – wbtcb.com

+ EasyCoin

Localbitcoins.com

## Jak ještě bitcoin získat

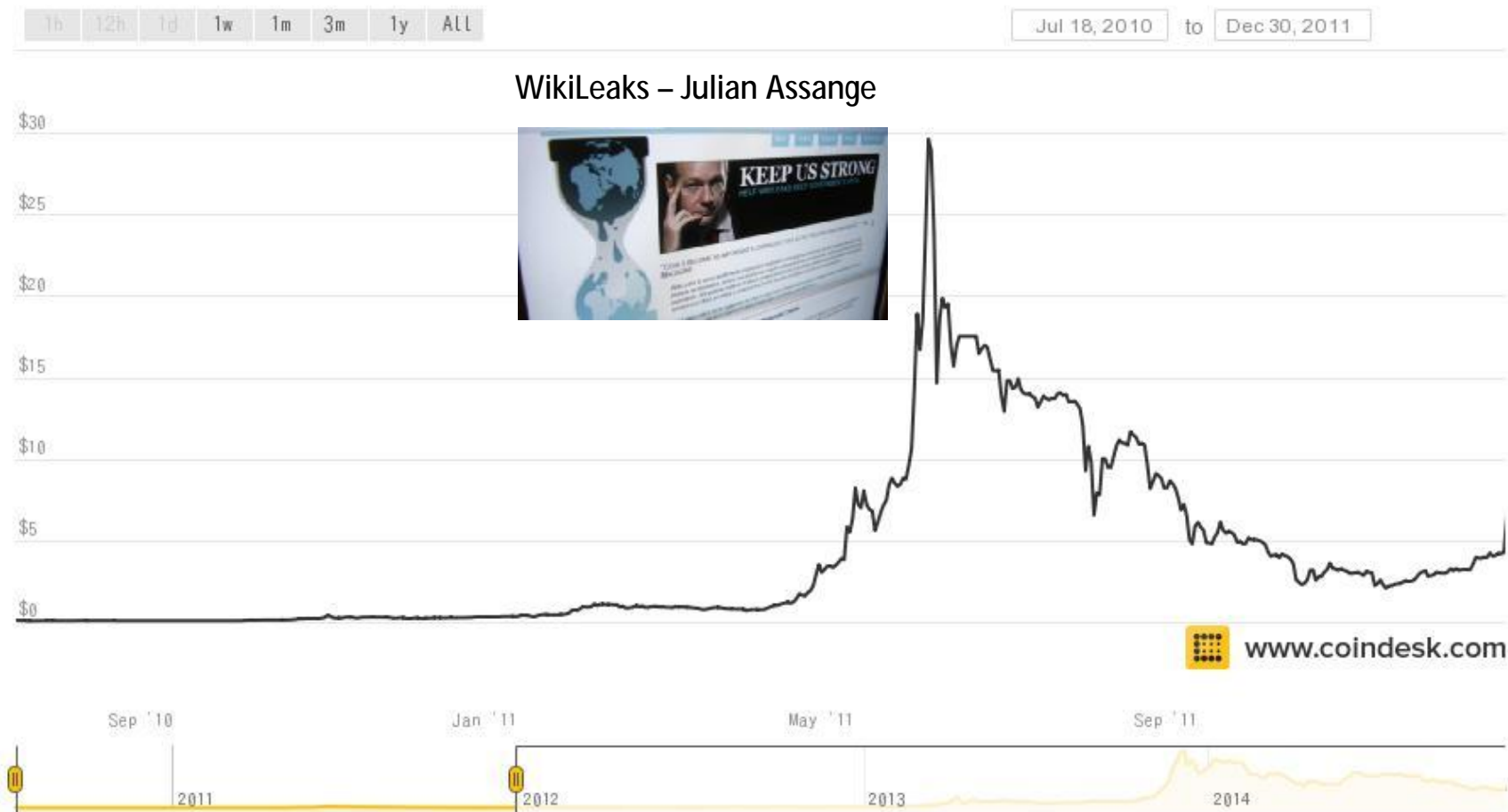
Mining

Prodej zboží a služeb

# Kurz bitcoinu, volatilita 2013-2014



# Kurz bitcoinu, volatilita - 2011



# Konec bitcoinu? Dnes 47x ...

**Forbes**

**New Posts**  
+2 posts this hour

**Most Popular**  
Why Companies Lose Talent

**Lists**  
Most Promising Companies

53

**Bitcoin  
Pronounced  
Dead In  
Forbes In  
June 2011**

1

 Share

87

 reddit

TECH 6/20/2011 @ 4:42AM 28,001 views

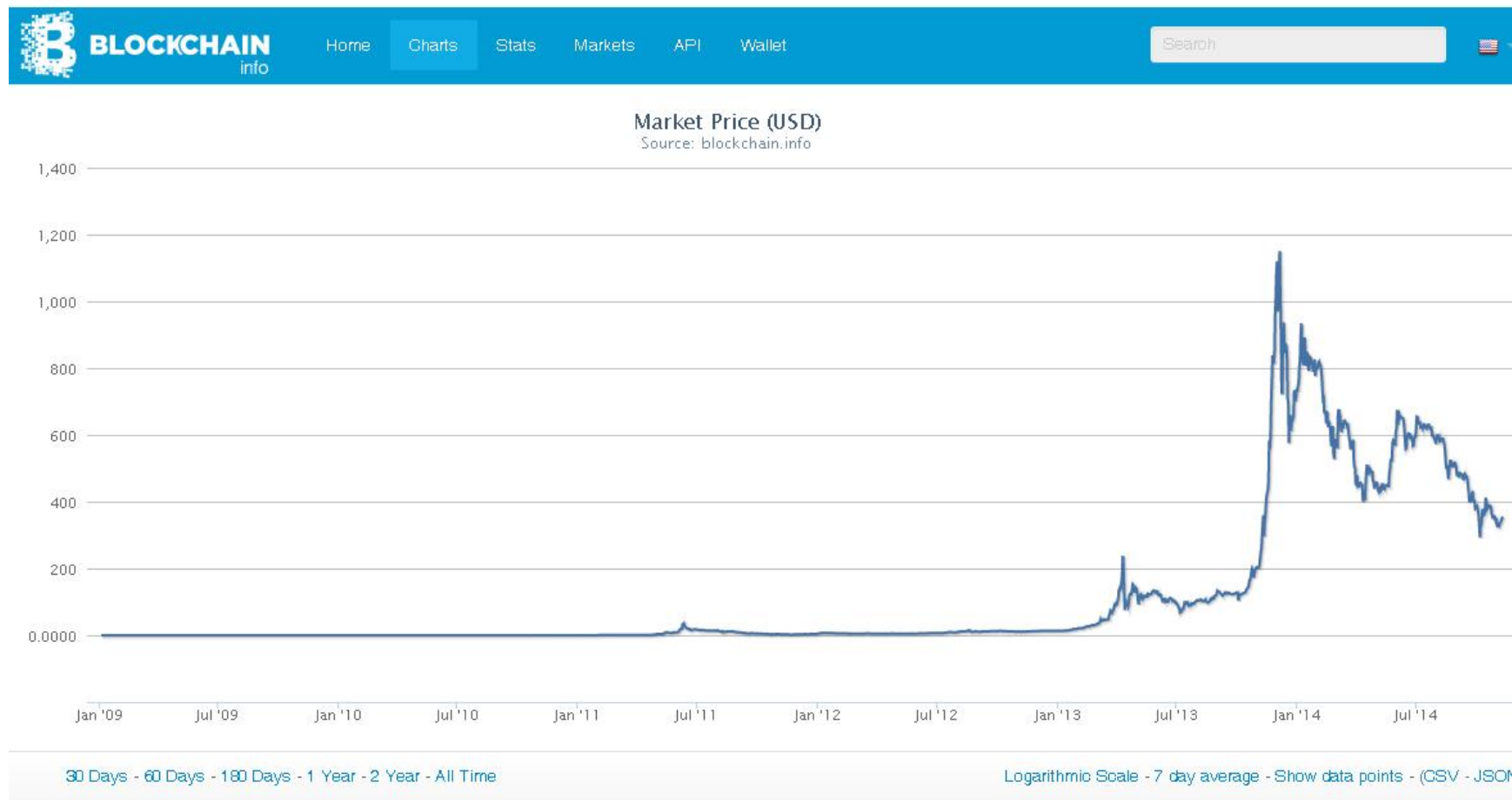
**So, That's the End of Bitcoin  
Then**

 47 comments, 5 called-out [+ Comment Now](#) [+ Follow Comments](#)

Or at least, this looks like it's the end of Bitcoin.

“ The Bitcoin community faced another crisis on Sunday afternoon as the price of the currency on the most popular exchange, Mt.Gox, fell from \$17 to pennies in a matter of minutes. Trading was quickly suspended and visitors to the home page were redirected to a statement blaming the crash on a compromised user account. Mt.Gox's Mark Karpeles said that the exchange would be taken offline to give administrators time to roll back the suspect transactions.

# Lineární graf 2009 - 2014



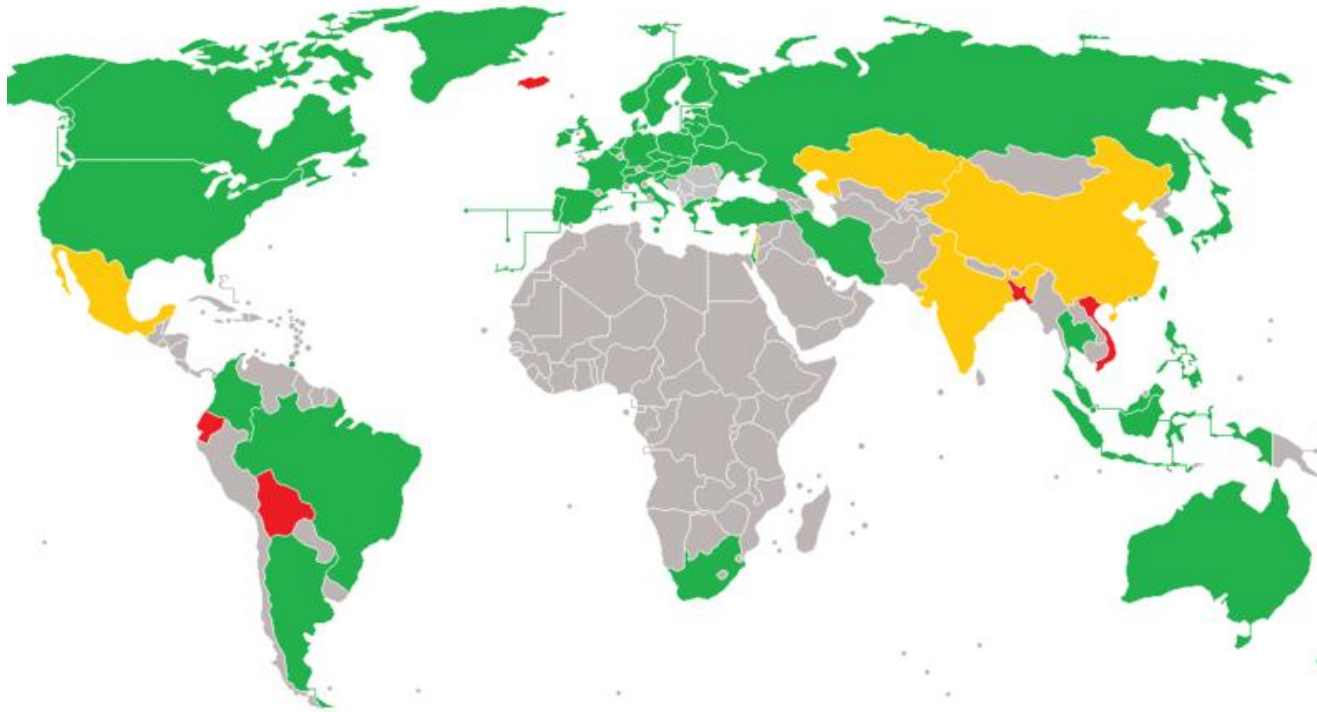
# Logaritmický graf 2010 - 2014





# Bitcoin a legislativa, regulace

- Bitcoin je v hledáčku zájmu donucovacích orgánů, daňových úřadů a právních regulátorů, z nichž všichni se snaží pochopit, jak kryptoměny zapadají do stávajících rámců. Zákonnost bitcoinových aktivit závisí na tom, kdo jste, kde žijete, a co s ním děláte.



# Bitcoin v České republice

ČNB – únor 2014: Nákup či prodej bitcoinů na vlastní účet nepředstavuje žádnou z platebních služeb podle § 3 odst. 1 ZPS ani bezhotovostní obchod s cizí měnou [§ 2 odst. 1 písm. e) ZPS].....

Obchodování s bitcoiny proto nevyžaduje povolení ČNB (takové povolení ČNB ani nemůže udělit) a nepodléhá dohledu ČNB. Z tohoto hlediska se neuplatní ani informační povinnosti vůči ČNB.

Povolení ČNB není potřebné ani k přijímání úhrad zboží a služeb prostřednictvím bitcoinů. Je však třeba upozornit, že soustavné odmítání tuzemských bankovek a mincí by mohlo naplnit znaky skutkové podstaty trestného činu ohrožování oběhu tuzemských peněz podle § 239 odst. 2 písm. a) trestního zákoníku, který stíhá toho, kdo bez zákonného důvodu odmítá tuzemské peníze.

- V ČR cca 100 akceptačních míst, Praha cca 50
- 8 bitcoinových bankomatů, 3 obousměrné
- WBTCB – EasyCoin – 8.000 míst Sazka a Česká pošta
- Paralelní Polis – bitcoinová kavárna, HUB, hackerspace
- silná BTC komunita
- Na špičce v technologiích – Slush pool, Trezor



[www.coinmap.org](http://www.coinmap.org)

# Budoucnost bitcoinu

- Příliv investic (VC) do rozvoje technologií a služeb  
2012 - 2 miliony USD 2013 - 93 mil. USD 2014 - 390 mil. USD
- Coinbase – leden 2014 – 75 milionů USD, březen 116 mil. USD
- Vznik nových (regulovaných) směnárů (Winklevoss – Gemini)
- Další akceptace BTC velkými společnostmi (nyní Dell, Microsoft, E-Bay, další na řadě je PayPal)
- E-shopy, obchody, restauracemi – nyní cca 100 tisíc míst
- Zlepšení uživatelské přívětivosti, důraz na bezpečnost
- Pokračování velké volatility na trzích, 200 – 2000 USD /1 rok (situace na trhu EUR/USD, hyperinflace - Ukrajina, Řecko?)
- Rozvoj nových technologií a měn na platformě blockchainu

# DOTAZY?

Další informace o bitcoinu

[www.cointelegraph.cz](http://www.cointelegraph.cz)

[www.btctip.cz](http://www.btctip.cz)

[www.paralelnipolis.cz](http://www.paralelnipolis.cz)



e-book zdarma – [www.btctip.cz](http://www.btctip.cz)